Carnegie Mellon
Software Engineering Institute

Pittsburgh, PA 15213-3890

Results from Conducting a CMMI[SM]-Based Risk Evaluation

Brian Gallagher

CMMI Technology Conference and User Group, 2001

Sponsored by the U.S. Department of Defense

Carnegie Mellon
Software Engineering Institute

Agenda

What is Risk?

What is Risk Management?

Why Manage Risk?

Using CMMI to Identify Risk

Using CMMI to Manage Risk

Summary

Carnegie Mellon
Software Engineering Institute

Agenda

- What is Risk?
- What is Risk Management?
- Why Manage Risk?
- Using CMMI to Identify Risk
- Using CMMI to Manage Risk
- Summary

Risk Defined[1]

Risk is the *potential* for realization of *unwanted negative consequences* of an event.

Rowe, William D. An Anatomy of Risk. Malabar, Fla.: Robert E. Krieger, 1988.

Risk is the measure of the *probability and severity* of *adverse effects.*

Lowrance, William W. Of Acceptable Risk. Los Altos, Ca.: William Kaufmann, 1976.

Risk is the *possibility of suffering loss.*

Webster's Third New International Dictionary. Springfield, Ma.: Merriam-Webster, 1981.

Carnegie Mellon
Software Engineering Institute

Risk Defined[2]

Risk is a *potential obstacle* to the successful completion of an endeavor

How would my risk differ if my endeavor were:

- driving from Miami to Las Vegas?
- walking across a busy street?
- digging a ditch?
- building a shed?
- developing a new space launch vehicle?
- fighting a battle?

Risk is NOT context-free! You can't know your risk until you know your endeavor

Carnegie Mellon
Software Engineering Institute

Agenda

What is Risk?

What is Risk Management?

Why Manage Risk?

Using CMMI to Identify Risk

Using CMMI to Manage Risk

Summary

Carnegie Mellon
Software Engineering Institute

Risk Management Defined

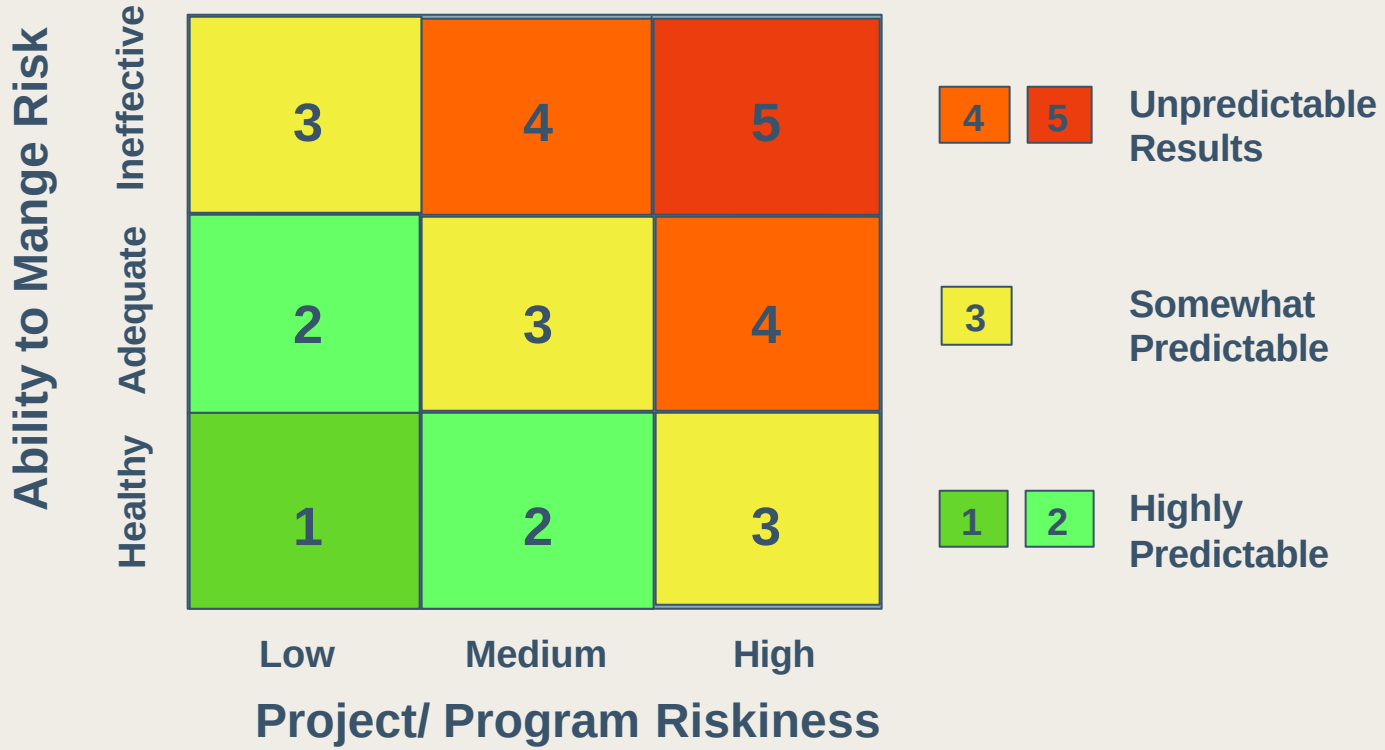
An *engineering practice* with processes, methods, and tools for managing risks in a development project

It provides a *disciplined environment for proactive decision making* to

- assess continually what could go wrong (risks)
- determine which risks are important to deal with
- implement strategies to deal with those risks

Two Key Concepts

- Knowing your risk
- Knowing your ability to manage risk



Carnegie Mellon
Software Engineering Institute

Agenda

What is Risk?

What is Risk Management?

Why Manage Risk?

Using CMMI to Identify Risk

Using CMMI to Manage Risk

Summary

Carnegie Mellon
Software Engineering Institute

Why Manage Risk?[1]

Developing new systems is still high risk:

- 49% of projects were *late and over budget*
- 28% were on time
- 23% were *cancelled before completion*

Source: 2000 Standish Group Chaos Report

Knowing what will cause you to fail, and acting before it happens, increases the odds of successfully delivering a system to the end-user

Carnegie Mellon
Software Engineering Institute

Why Manage Risk?[2]

One shared characteristic of failed projects is the inability of project members to communicate potential problems to the decision makers within a project.

- 72% of failed projects had team members who knew of impending doom.
- Only 19% of the project managers on the same projects shared the insight.

Source: Robert Glass – Software Runaways

Risk management allows team members to discuss potential problems in a structured, non-threatening manner providing insight to decision makers.

Carnegie Mellon
Software Engineering Institute

Risk Management Required in DoD Policy

DoDR 5002-R: *Mandatory Procedures for Major Defense Acquisition Programs (MDAPS) and Major Automated Information System (MAIS) Acquisition Programs*

- Requires risk assessment and risk reduction throughout an acquisition
- Specifically, section C.5 RISK: "The PM shall identify the risk areas of the program and integrate risk management within overall program management"

Carnegie Mellon
Software Engineering Institute

Risk Management Required in Standards[1]

ISO 9001: *Quality systems - Model for quality assurance in design/development, production, installation and servicing* (section 4-14)

ISO-IEC DTR 15504-2: *Information Technology - Software Process Assessment Part 2: A Reference Model For Processes and Process Capability* (section 5.3 of working draft)

Carnegie Mellon
Software Engineering Institute

Risk Management Required in Standards[2]

IEEE

- 7-4.3.2: *IEEE Standard Criteria for Digital Computers in Safety Systems of Nuclear Power Generating Stations* (will be in next revision)
- P1448 - EIA PN3764: US Implementation of ISO/IEC 12207 *Standard for Information Technology - Software life cycle processes* (section G.8)
- P1540: *Standard for Software Life Cycle Processes—Risk Management*

Carnegie Mellon
Software Engineering Institute

Risk Management Required in Maturity Models[1]

- Software Acquisition Capability Maturity Model® (SA-CMM) — *Acquisition Risk Management* Key Process Area
- Systems Engineering Capability Maturity Model® (SE-CMM) — *Risk Management* focus area
- Capability Maturity Model® for Software (SW-CMM) — Risk management is an *expected activity* in *Software Project Planning* and *Software Project Tracking and Oversight* Key Process Areas at Level 2, *Integrated Software Management* KPA at Level 3

* Capability Maturity Model and CMM are registered in the U.S. Patent and Trademark Office.

Carnegie Mellon
Software Engineering Institute

Risk Management Required in Maturity Models[2]

- Capability Maturity Model® - Integrated (CMMI℠-SE/SW/IPPD/A)
  - Risk Management Practices in *Project Planning* and *Project Monitoring and Control* Process Areas
  - *Risk Management* is a separate Process Area

CMMI is a Service Mark of Carnegie Mellon University

Carnegie Mellon
Software Engineering Institute

Agenda

What is Risk?

What is Risk Management?

Why Manage Risk?

Using CMMI to Identify Risk

Using CMMI to Manage Risk

Summary

Carnegie Mellon
Software Engineering Institute

Risk Identification

The most difficult part of managing risk is *finding them in the first place*

Risks must be identified *continually* throughout the development lifecycle.

- Early risk identification allows managers to build plans based on mitigation of high risk areas – especially vital in an iterative or evolutionary development approach.
- Continuous risk identification allows managers to adjust plans as risk evolves.

Carnegie Mellon
Software Engineering Institute

Using CMMI to Identify Risk[1]

CMMI Appraisals – Using the CMMI as a yardstick against which the organization's practices are judged for compliance.

- Need CMMI and assessment trained team and prepared participants
- Potentially adversarial because "*experts*" *determine risk* (non-compliance) based on CMMI practices

Risks are identified *implicitly*

Carnegie Mellon
Software Engineering Institute

Using CMMI to Identify Risk$_2$

CMMI-based Risk Assessment – Using the CMMI as a "taxonomy" to discuss the project's or organization's practices.

- Need a "Picture of Success", *smart team members*, and *willing participants*
- Less adversarial because *project members determine risk* based on CMMI practices

Risks are identified *explicitly*

Carnegie Mellon
Software Engineering Institute

Example

Program X is a space-based system designed to upgrade processing of an existing sensor system and replace the sensors with new space sensors.

Has a ground component and a space component.

Ground portion had an Acquisition Program Baseline breach.

An independent team performed a risk assessment in FEB 2000 at the request of the Program Element Officer (PEO) and a follow-up risk assessment at the program's request in FEB 2001

Carnegie Mellon
Software Engineering Institute

What we did in 2000 1

Assessment refocused from typical *red team* activity to a risk assessment

Team asked the PEO to articulate a "*Picture of Success*"

Risk assessments performed at operational site and development site

Purpose: Identify obstacles to successful achievement of the PEO's "*Picture of Success*" – Results used by PEO to brief Senior Acquisition Executives

Carnegie Mellon
Software Engineering Institute

What we did in 2000 $_2$

The *Picture of Success* as articulated by PEO on 1 FEB 00:

Successful certification of Increment 1 on the mutually agreed upon restructure date

- ***Successful entry into IOT&E***
- ***Sound approach established for mitigating Increment 1 impacts and successfully executing Increment 2***

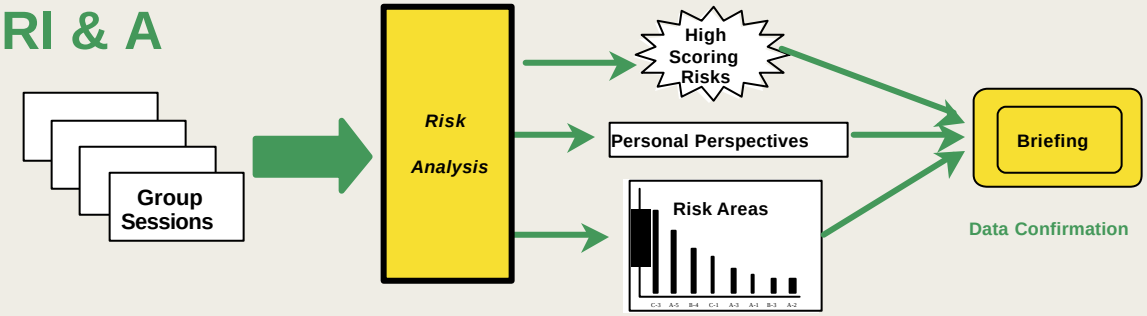
Carnegie Mellon
Software Engineering Institute

What we did in 2000 3

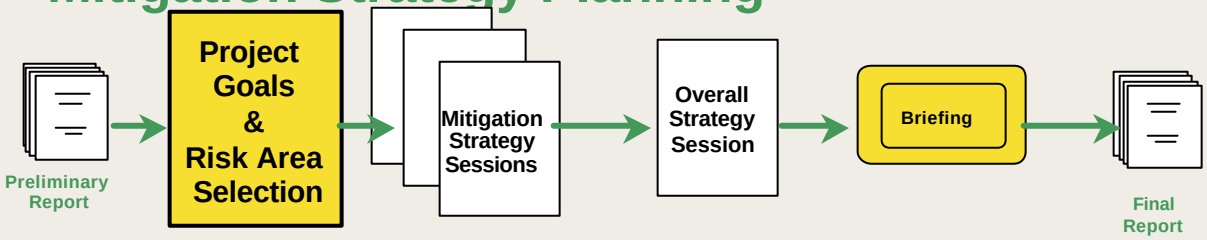
- 7 interview sessions
- 31 people participated
- 169 risk statements captured
- 15 risk areas defined

The Software Risk Evaluation Process 1

RI & A

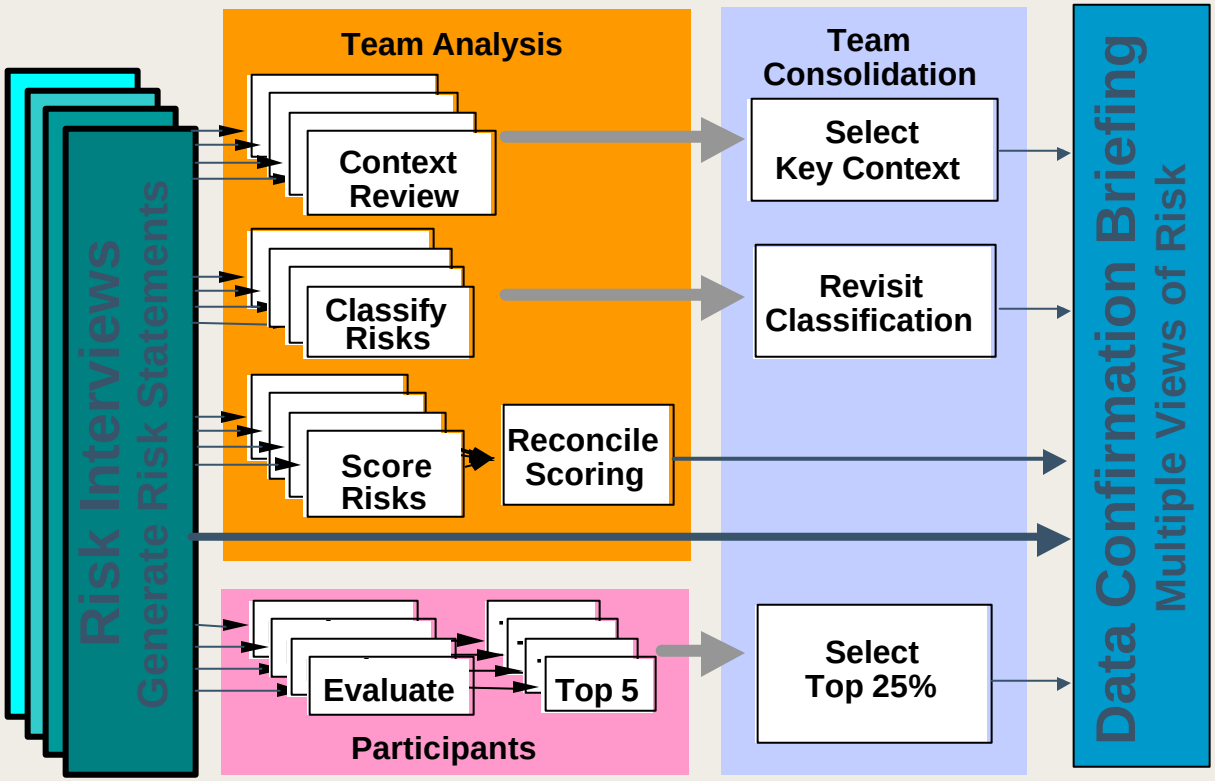


Mitigation Strategy Planning

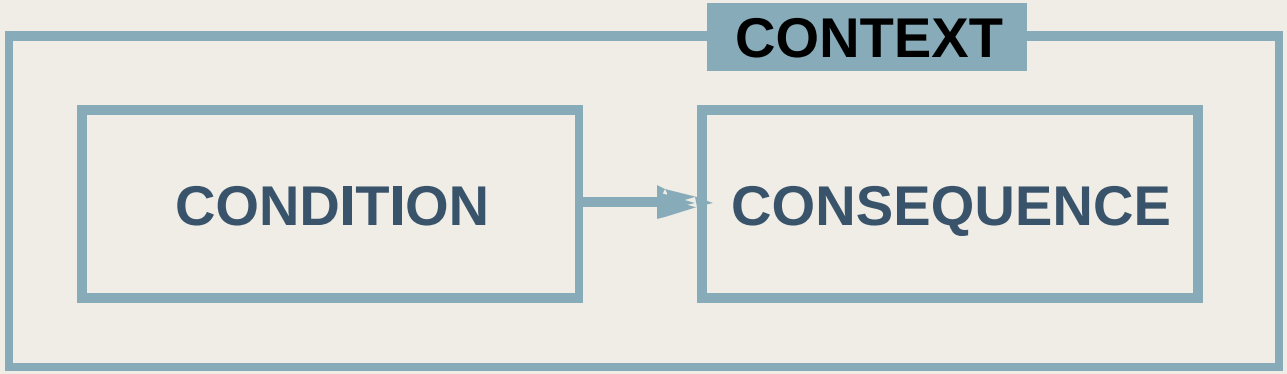


RI&A - risk identification and analysis

The Software Risk Evaluation Process 2



The Software Risk Evaluation Process 3



Condition: something that is true today
Consequence: something that may occur in the future as a result of that condition

Examples:

We don't trace requirements from source to implementing component; may not be able to prove we meet the user's expectations.

COTS high-speed datalink never envisioned by vendor to be used in hardened environment; may not perform as needed, causing re-work and integration slips.

Carnegie Mellon
Software Engineering Institute

What We Did 2001$_1$

Ground cost estimates in question

Desire to raise maturity of ground organization to increase confidence in plans

High level Air Force officials desire developer to operate at Maturity Level 4 of the Software Capability Maturity Model (SW-CMM)

Carnegie Mellon
Software Engineering Institute

What We Did 2001_2

Assessment refocused from SW-CMM "*check the box*" activity to a risk assessment

Team asked sponsor to articulate a "*Picture of Success*"

Team performed risk assessments at Prime, Sub, and Government program office

Purpose: Identify obstacles to successful achievement of the Program's "*Picture of Success*" – program will use results to improve their own practices

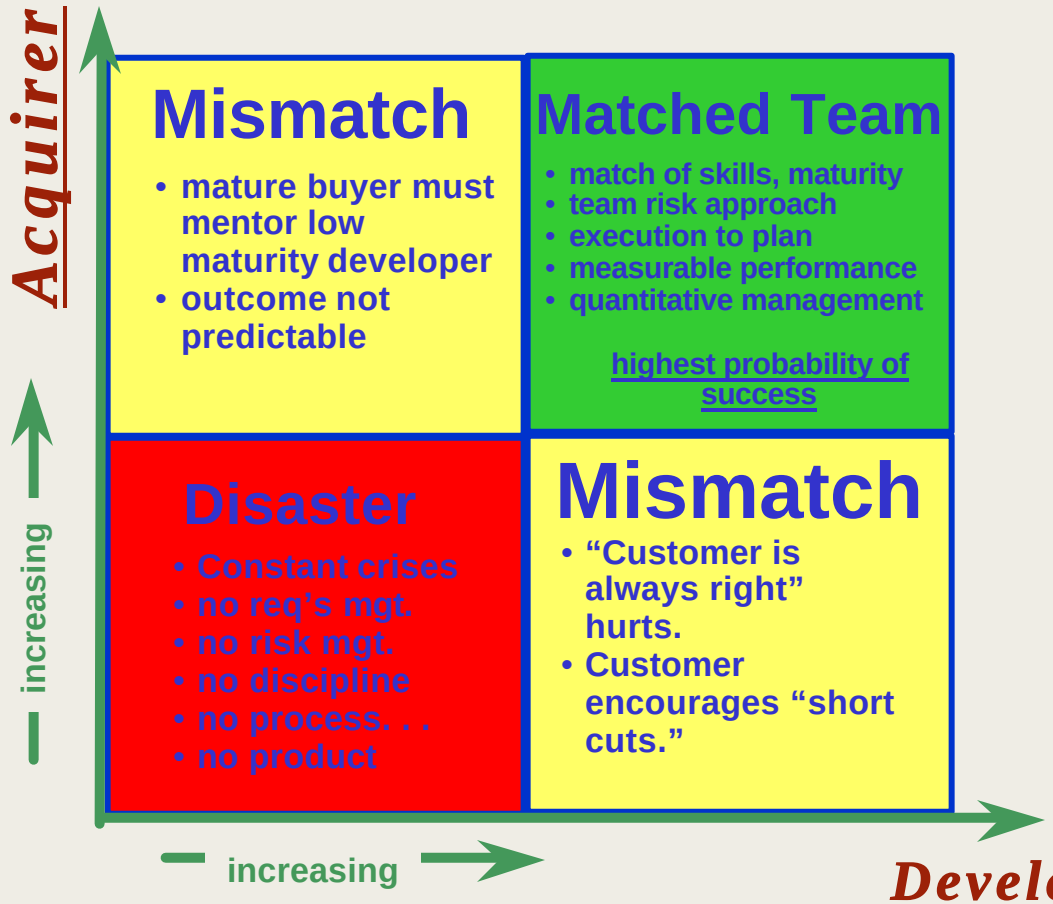
Carnegie Mellon
Software Engineering Institute

What We Did 2001_3

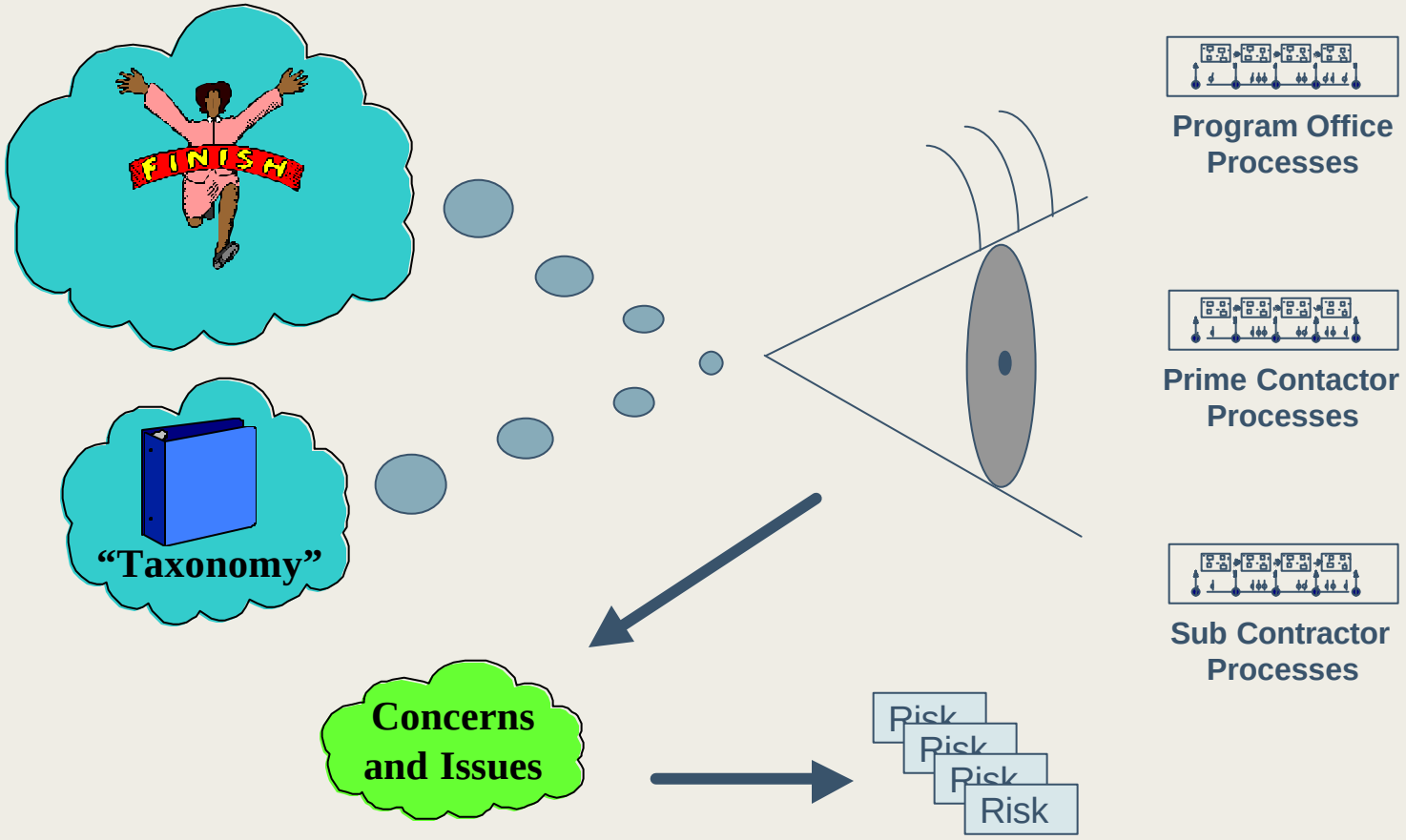
The *Picture of Success* as confirmed by sponsor:

The ground team is a world-class acquisition and development organization delivering high quality products and services on the first promised date, within cost constraints, containing all required functionality

A Look at Maturity



Scope of this Risk Evaluation



Carnegie Mellon
Software Engineering Institute

Our Development "Taxonomy"

Category	Process Areas
Project Management	Project Planning Project Monitoring and Control Supplier Agreement Management Integrated Project Management Risk Management Integrated Teaming Quantitative Project Management
Support	Configuration Management Process and Product Quality Assurance Measurement and Analysis Decision Analysis and Resolution Causal Analysis and Resolution
Engineering	Requirements Management Requirements Development Technical Solution Product Integration Verification Validation
Process Management	Organizational Process Focus Organizational Process Definition Organizational Training Organizational Environment for Integration Organizational Process Performance Organizational Innovation and Deployment

Risk Topic 1: Project Planning

1. How does your *project* establish and maintain plans that define the project activities?

CMMI PA: PP - Project Planning (Maturity Level 2, Category: Project Management)

Probing Questions:

- (GO) How does your project establish the planning parameters (e.g., guidelines and constraints) for estimating effort and cost of its development activities? Is historical data used?
- (GO) How does your project establish and maintain its plans?
- (GO) How does your project obtain commitments to the project plan? How are these maintained?
- (GO) How does your project ensure that project planning is institutionalized as a managed process?
- How does your project perform replanning?
- How does your project plan for the identification and analysis of risk?

CMMI Practices:

Are there risks associated with the way the project tries to:

- Estimate the Scope of the Project
- Establish Estimates of Project Attributes
- Define Project Life Cycle
- Determine Estimates of Effort and Cost
- Establish the Budget and Schedule
- Identify Project Risks
- Plan for Data Management
- Plan for Project Resources
- Plan for Needed Knowledge and Skills
- Plan Stakeholder Involvement
- Establish the Project Plan
- Review Subordinate Plans
- Reconcile Work and Resource Levels
- Obtain Plan Commitment

Additional Topics:

Potential Sources of Risk:

- ❑ Project plans:
  - ❑ QA ❑ SCM ❑ CM ❑ M&A
- ❑ Estimation models/Results/BOE
- ❑ Evidence of Adequate Resources and Tools
- ❑ Project schedules and/or dependencies
- ❑ WBS
- ❑ Management training for planning
- ❑ People assigned responsibility and trained
- ❑ Risk Identification/Analysis
- ❑ Task planning
- ❑ Coordinate with stakeholders

Carnegie Mellon
Software Engineering Institute

Example Risk Statements

Schedules are based on productivity rates that are 50% higher than historically experienced; we are unlikely to meet our schedule

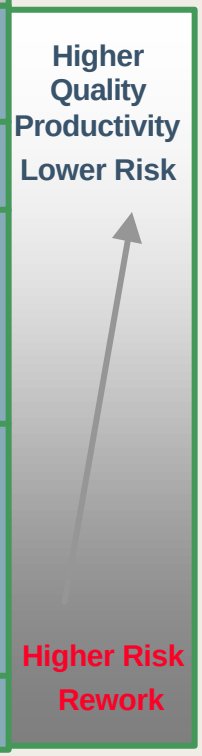
Non-software development activities (e.g. OPS concepts, requirements development) are not counted in productivity numbers; productivity estimates may be skewed

Commitments on part of the Government are not being fulfilled; additional unplanned effort expended

Cost, schedule, and technical baselines are all fixed and we don't know the priorities; we may not be able to propose effective alternatives

Our Acquisition "Taxonomy"

Level	Focus	Key Process Areas
5 Optimizing	*Continuous process improvement*	Acquisition Innovation Management Continuous Process Improvement
4 Quantitative	*Quantitative management*	Quantitative Acquisition Management Quantitative Process Management
3 Defined	*Process standardization*	Training Program Acquisition Risk Management Contract Performance Management Project Performance Management Process Definition and Maintenance
2 Repeatable	*Basic project management*	Transition to Support Evaluation Contract Tracking and Oversight Project Management Requirements Development and Mgt. Solicitation Software Acquisition Planning
1 Initial	*Competent people and heroics*	



Risk Topic 4: Project Management

4. How does your *project* manage the activities of the project office and supporting organizations to ensure a timely, efficient, and effective software acquisition?

SA-CMM PA: PM – Project Management (Maturity Level 2)

Probing Questions:

- (GO) How are project management activities are planned, organized, controlled, and communicated?
- (GO) Describe how the performance, cost, and schedule objectives of the software acquisition project are measured and controlled throughout the software acquisition?
- (GO) Are problems discovered during the software acquisition managed and controlled?
- How does your project ensure that all appropriate resources are included in identifying, negotiating, and tracking critical dependencies?
- How are issues resolved among all project functions?

SA-CMM Practices:

Are there risks associated with the way the project implements these practices?

- The project team performs its activities in accordance with its documented software acquisition management plans.
- The roles, responsibilities, and authority for the project functions are documented, maintained, and communicated to affected groups.
- The project team's commitments, and changes to commitments, are communicated to affected groups.
- The project team tracks the risks associated with cost, schedule, resources, and the technical aspects of the project.
- The project team tracks project issues, status, execution, funding, and expenditures against project plans and takes action.
- The project team implements a corrective action system for the identification, recording, tracking, and correction of problems discovered during the software acquisition.
- The project team keeps its plans current during the life of the project as replanning occurs, issues are resolved, requirements are changed, and new risks are discovered.

Additional Topics:

Potential Sources of Risk:

- ❑ Project team follows plans
- ❑ Roles clearly defined and communicated
- ❑ Commitments documented and managed
- ❑ Project team honors commitments
- ❑ GFE or other dependencies managed
- ❑ Risks are tracked
- ❑ Earned value
- ❑ Action item databases
- ❑ Schedules for collaborative activities

Carnegie Mellon
Software Engineering Institute

Example Risk Statements

Number, experience level, and quality of SPO systems engineering staff is low; unable to do everything that is needed

We have stovepiped the systems engineering functions within the SPO; things may not fit together

The requirements set is a compromise to satisfy many users and is driving the design; the users may not even want to operate the system as specified

There are no documented acquisition processes; may spend valuable time figuring out what to do instead of doing it

Carnegie Mellon
Software Engineering Institute

Combined Results

- 16 interview sessions
- 74 people participated
- 476 risk statements captured
- 153 risk statements (32%) rated as top risks by the team
- 145 risk statements (30%) rated as “#1” through “#3” by the people who were interviewed (“participants”)
- Risk Areas
  - 11 risk areas at Prime
  - 9 risk areas at Sub
  - 12 risk areas at program office
- Combined into 8 “program” risk areas

Carnegie Mellon
Software Engineering Institute

Combined Risk Areas

Immature Development & Acquisition Processes

Inadequate Systems Engineering

Strained Resources

Contractor Management

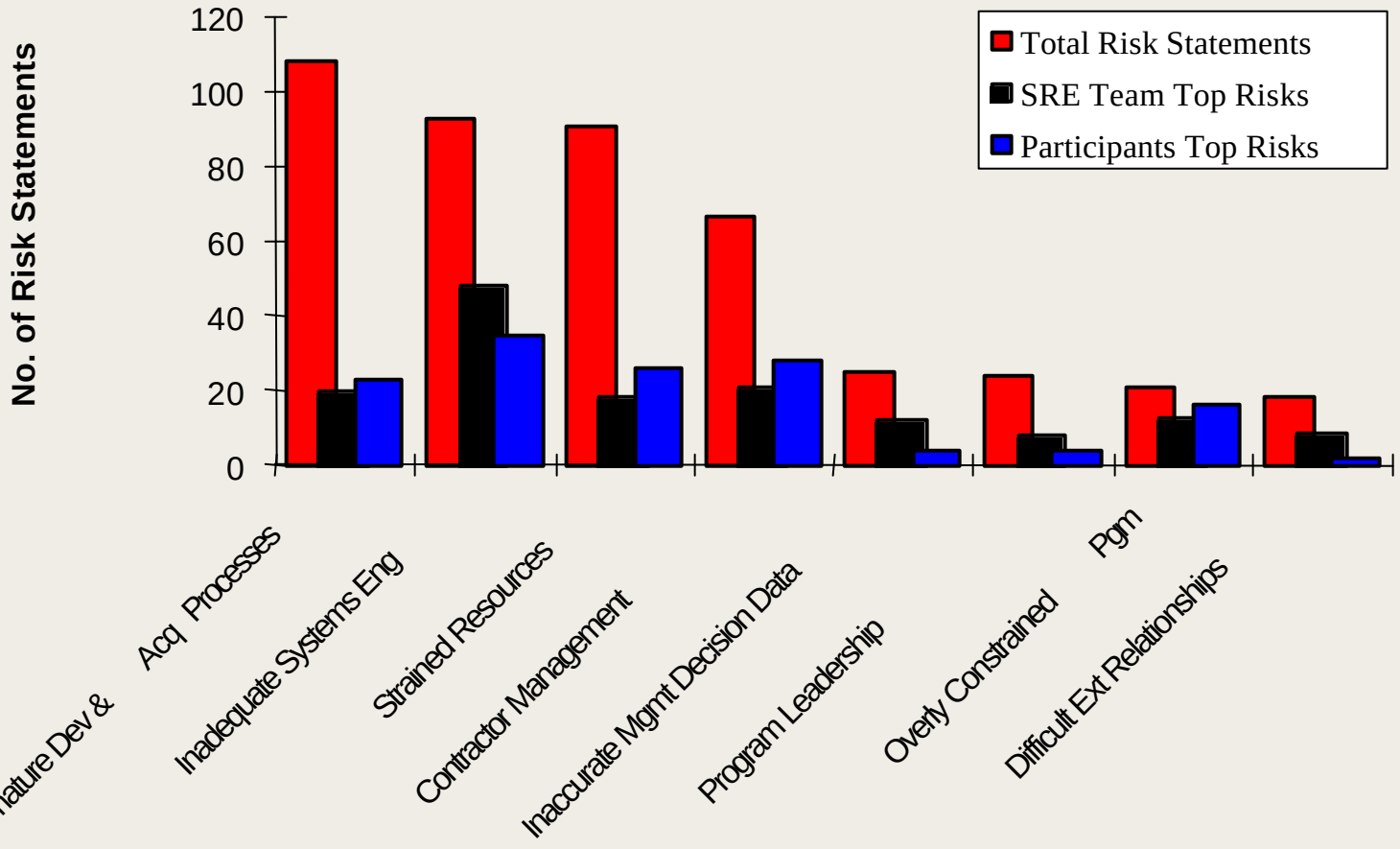
Inaccurate Management Decision Data

Program Leadership

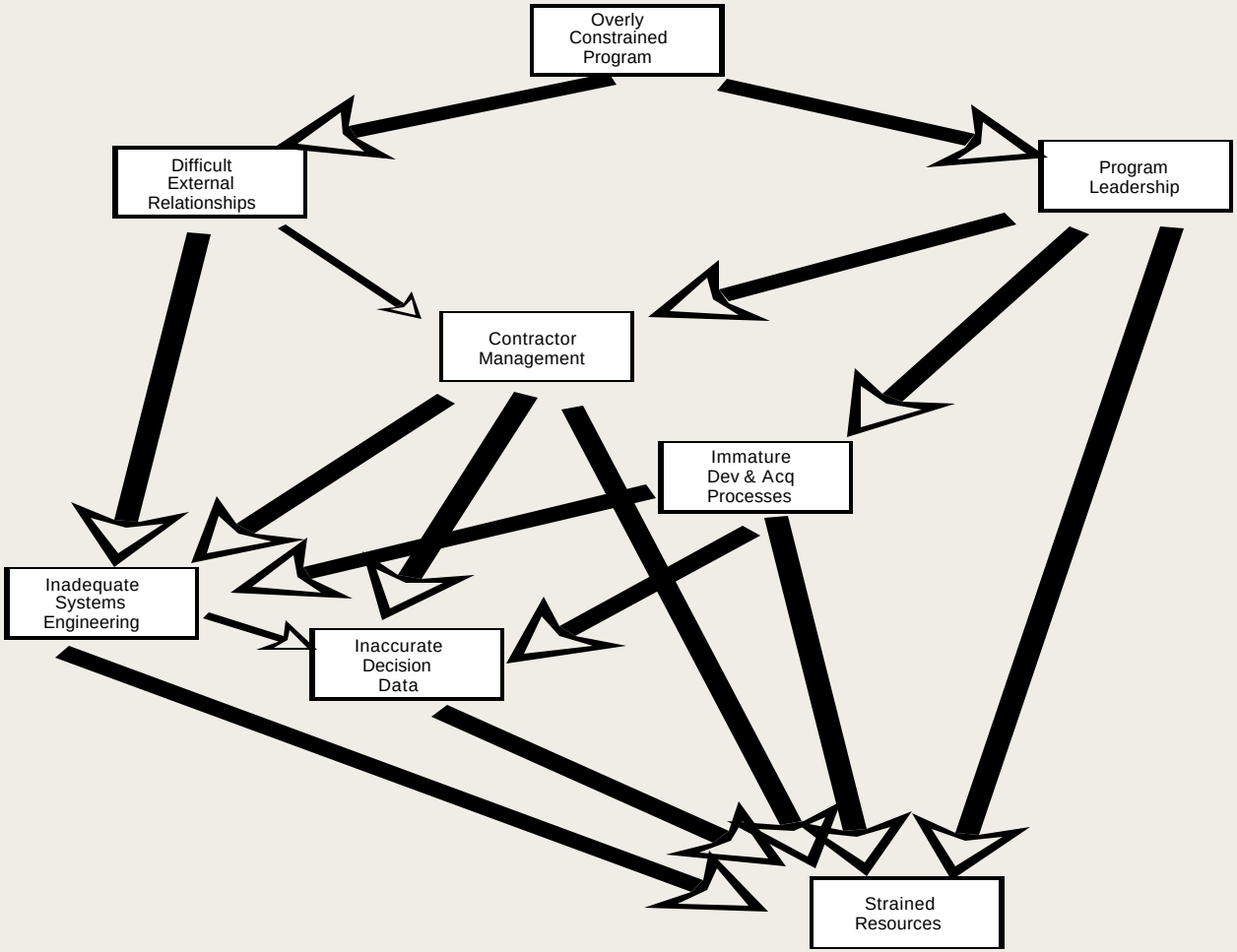
Overly Constrained Program

Difficult External Relationships

Risk Statements per Risk Area



Combined Results



Carnegie Mellon
Software Engineering Institute

Recommendations

Highly Difficult but High Payback in Mitigating:

- Overly Constrained Program
- Difficult External Relationships

Must address leadership issues - leadership involvement needed to mitigate these risk areas

Conduct Mitigation Strategy Planning Sessions (MSP) for:

- Inadequate Systems Engineering
- Immature Dev. & Acq. Processes
- Inaccurate Management Decision Data

Mitigating risk areas above coupled with addressing Low Hanging Fruit help mitigate Strained Resources

Carnegie Mellon
Software Engineering Institute

Agenda

What is Risk?

What is Risk Management?

Why Manage Risk?

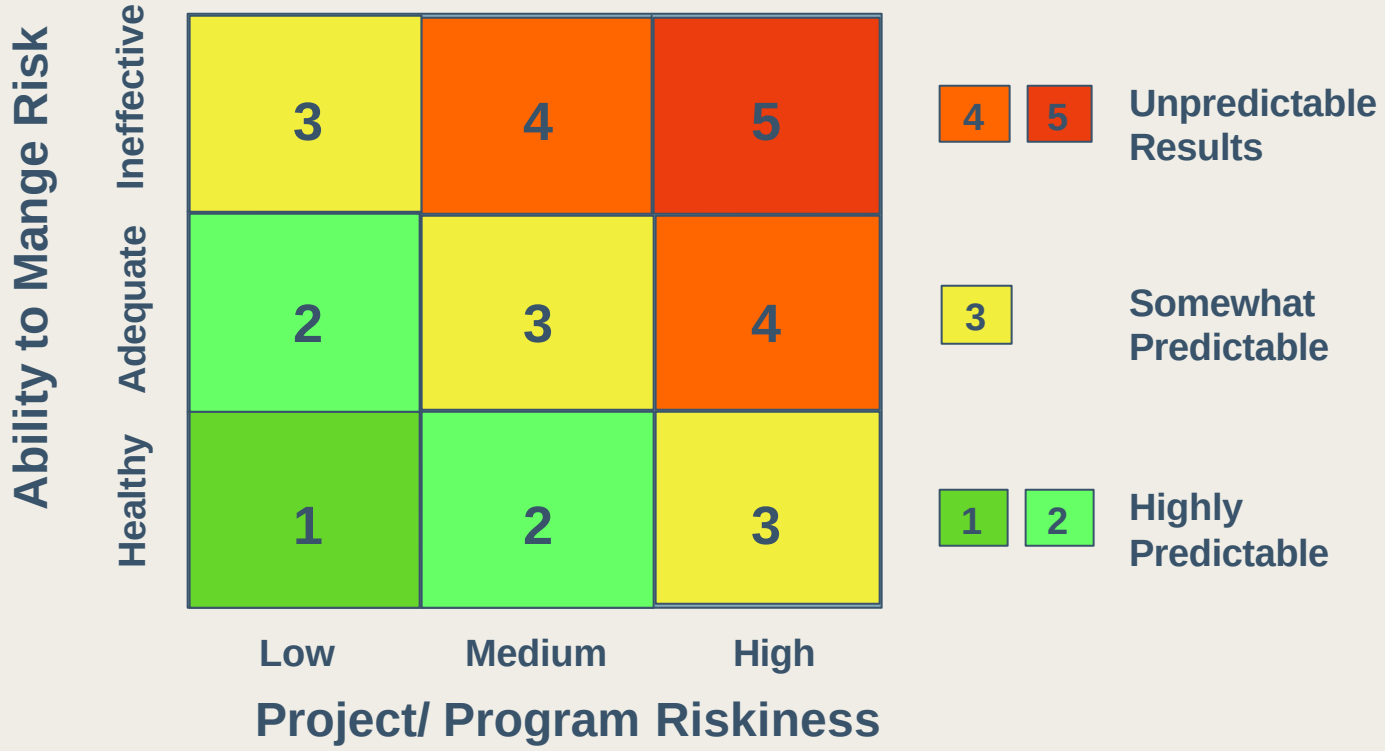
Using CMMI to Identify Risk

Using CMMI to Manage Risk

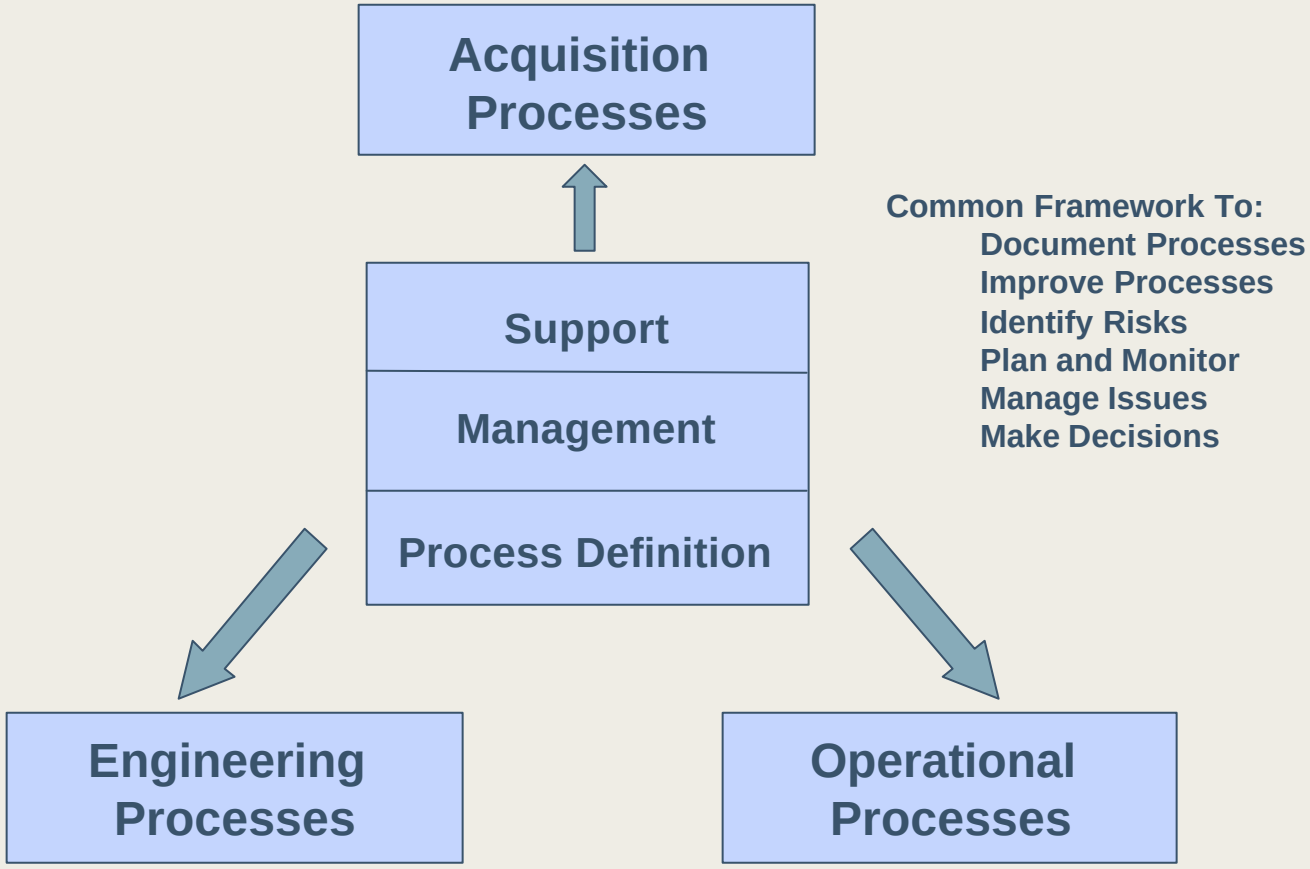
Summary

Key Concepts Revisited

- Knowing your risk
- Knowing your ability to manage risk



CMMI as a Framework to Manage Risk



Common Framework To:

- Document Processes
- Improve Processes
- Identify Risks
- Plan and Monitor
- Manage Issues
- Make Decisions

Carnegie Mellon
Software Engineering Institute

Agenda

What is Risk?

What is Risk Management?

Why Manage Risk?

Using CMMI to Identify Risk

Using CMMI to Manage Risk

Summary

Carnegie Mellon
Software Engineering Institute

Summary

Risk is a potential obstacle to the success of an endeavor

The CMMI can be used to identify those obstacles implicitly (CMMI Appraisals) or explicitly (CMMI-based Risk Assessment)

A CMMI-based Risk Assessment can start to introduce the CMMI model in an organization

The CMMI can be used to increase an organization's ability to manage risk

Carnegie Mellon
Software Engineering Institute

Contact Information

For more information on CMMI, CMMI Appraisals, or CMMI-based Risk Assessments, contact:

Customer Relations
customer-relations@sei.cmu.edu

or

Brian Gallagher
bg@sei.cmu.edu

412-268-7157